Vendor: CISCO

Exam Code: 642-618

Exam Name: Deploying Cisco ASA Firewall Solutions (FIREWALL) V2.0
QUESTION 1
When enabling a Cisco ASA to send syslog messages to a syslog server, which syslog level will produce the most messages?

A. notifications
B. informational
C. alerts
D. emergencies
E. errors
F. debugging

Answer: F

QUESTION 2
Refer to the exhibit.

```
class-map http
   match port tcp eq 21
class-map ftp
   match port tcp eq 21
policy-map test
   class http
       inspect http
   class ftp
       inspect ftp
```

Which statement about the policy map named test is true?

A. Only HTTP inspection will be applied to the TCP port 21 traffic.
B. Only FTP inspection will be applied to the TCP port 21 traffic.
C. both HTTP and FTP inspections will be applied to the TCP port 21 traffic.
D. No inspection will be applied to the TCP port 21 traffic, because the http class map configuration conflicts with the ftp class map.
E. All FTP traffic will be denied, because the FTP traffic will fail the HTTP inspection.

Answer: B
QUESTION 3
In which type of environment is the Cisco ASA MPF set connection advanced-options tcp-state- bypass option the most useful?

A. SIP proxy
B. WCCP
C. BGP peering through the Cisco ASA
D. asymmetric traffic flow
E. transparent firewall

Answer: D

QUESTION 4
By default, how does the Cisco ASA authenticate itself to the Cisco ASDM users?

A. The administrator validates the Cisco ASA by examining the factory built-in identity certificate thumbprint of the Cisco ASA.
B. The Cisco ASA automatically creates and uses a persistent self-signed X.509 certificate to authenticate itself to the administrator.
C. The Cisco ASA automatically creates a self-signed X.509 certificate on each reboot to authenticate itself to the administrator.
D. The Cisco ASA and the administrator use a mutual password to authenticate each other.
E. The Cisco ASA authenticates itself to the administrator using a one-time password.

Answer: C

QUESTION 5
Which flag shown in the output of the show conn command is used to indicate that an initial SYN packet is from the outside (lower security-level interface)?
QUESTION 6
Which statement about the default ACL logging behavior of the Cisco ASA is true?

A. The Cisco ASA generates system message 106023 for each denied packet when a deny ACE is configured.
B. The Cisco ASA generates system message 106023 for each packet that matched an ACE.
C. The Cisco ASA generates system message 106100 only for the first packet that matched an ACE.
D. The Cisco ASA generates system message 106100 for each packet that matched an ACE.
E. No ACL logging is enabled by default.

Answer: A

QUESTION 7
In one custom dynamic application, the inside client connects to an outside server using TCP port 4444 and negotiates return client traffic in the port range of 5000 to 5500. The

ASA5520# show conn
29 in use, 63 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22 bytes 1774 flags UIO <output omitted>
server then starts streaming UDP data to the client on the negotiated port in the specified range. Which Cisco ASA feature or command supports this custom dynamic application?

A. TCP normalizer  
B. TCP intercept  
C. ip verify command  
D. established command  
E. tcp-map and tcp-options commands  
F. set connection advanced-options command

**Answer: D**

**QUESTION 8**
Which Cisco ASA CLI command is used to enable HTTPS (Cisco ASDM) access from any inside host on the 10.1.16.0/20 subnet?

A. http 10.1.16.0 0.0.0.0 inside  
B. http 10.1.16.0 0.0.15.255 inside  
C. http 10.1.16.0 255.255.240.0 inside  
D. http 10.1.16.0 255.255.255.255

**Answer: C**

**QUESTION 9**
Which statement about SNMP support on the Cisco ASA appliance is true?

A. The Cisco ASA appliance supports only SNMPv1 or SNMPv2c.  
B. The Cisco ASA appliance supports read-only and read-write access.  
D. The Cisco ASA appliance can send SNMP traps to the network management station only using SNMPv2.
QUESTION 10
On Cisco ASA Software Version 8.4.1 and later, when you configure the Cisco ASA appliance in transparent firewall mode, how is the Cisco ASA management IP address configured?

A. using the IP address global configuration command  
B. using the IP address GigabitEthernet 0/x interface configuration command  
C. using the IP address BVI x interface configuration command  
D. using the bridge-group global configuration command  
E. using the bridge-group GigabitEthernet 0/x interface configuration command  
F. using the bridge-group BVI x interface configuration command  

Answer: C

QUESTION 11
A Cisco ASA appliance running software version 8.4.1 has an active botnet traffic filter license with 1 month left on the time-based license. Which option describes the result if a new botnet traffic filter with a 1 year time-based license is activated also?

A. The time-based license for the botnet traffic filter is valid only for another month.  
B. The time-based license for the botnet traffic filter is valid for another 12 months.  
C. The time-based license for the botnet traffic filter is valid for another 13 months.  
D. The new 1 year time-based license for the botnet traffic filter cannot be activated until the current botnet traffic filter license expires in a month.

Answer: C

QUESTION 12
In the default global policy, which traffic is matched for inspections by default?

A. match any
B. match default-inspection-traffic
C. match access-list
D. match port
E. match class-default

Answer: B

**QUESTION 13**
Which additional active/standby failover feature was introduced in Cisco ASA Software Version 8.4?

A. HTTP stateful failover
B. OSPF and EIGRP routing protocol stateful failover
C. SSL VPN stateful failover
D. IPsec VPN stateful failover
E. NAT stateful failover

Answer: B

**QUESTION 14**
On the Cisco ASA, where are the Layer 5-7 policy maps applied?

A. inside the Layer 3-4 policy map
B. inside the Layer 3-4 class map
C. inside the Layer 5-7 class map
D. inside the Layer 3-4 service policy
E. inside the Layer 5-7 service policy

Answer: A

**QUESTION 15**
Refer to the exhibit.
Which command options represent the inside local address, inside global address, outside local address, and outside global address?

A. 1 = outside local, 2 = outside global, 3 = inside global, 4 = inside local 
B. 1 = outside local, 2 = outside global, 3 = inside local, 4 = inside global 
C. 1 = outside global, 2 = outside local, 3 = inside global, 4 = inside local 
D. 1 = inside local, 2 = inside global, 3 = outside global, 4 = outside local 
E. 1 = inside local, 2 = inside global, 3 = outside local, 4 = outside global 

Answer: D

QUESTION 16
Which Cisco ASDM 6.4.1 pane is used to enable the Cisco ASA appliance to perform TCP checksum verifications?

A. Configuration > Firewall > Service Policy Rules 
B. Configuration > Firewall > Advanced > IP Audit > IP Audit Policy 
C. Configuration > Firewall > Advanced > IP Audit > IP Audit Signatures 
D. Configuration > Firewall > Advanced > TCP options 
E. Configuration > Firewall > Objects > TCP Maps 
F. Configuration > Firewall > Objects > Inspect Maps 

Answer: E

QUESTION 17
Refer to the exhibit.
Which two statements about the class maps are true? (Choose two.)

A. These class maps are referenced within the global policy by default for HTTP inspection.
B. These class maps are all type inspect http class maps.
C. These class maps classify traffic using regular expressions.
D. These class maps are Layer 3/4 class maps.
E. These class maps are used within the inspection_default class map for matching the default inspection traffic.

Answer: BC

QUESTION 18
Which five options are valid logging destinations for the Cisco ASA? (Choose five.)

A. AAA server
B. Cisco ASDM
C. buffer
D. SNMP traps
E. LDAP server
F. email
G. TCP-based secure syslog server
**QUESTION 19**
When troubleshooting a Cisco ASA that is operating in multiple context mode, which two verification steps should be performed if a user context does not pass user traffic? (Choose two.)

A. Verify the interface status in the system execution space.
B. Verify the mac-address-table on the Cisco ASA.
C. Verify that unique MAC addresses are configured if the contexts are using nonshared interfaces.
D. Verify the interface status in the user context.
E. Verify the resource classes configuration by accessing the admin context.

**Answer:** AD

**QUESTION 20**
On the Cisco ASA Software Version 8.4.1, which three parameters can be configured using the set connection command within a policy map? (Choose three.)

A. per-client TCP and/or UDP idle timeout
B. per-client TCP and/or UDP maximum session time
C. TCP sequence number randomization
D. maximum number of simultaneous embryonic connections
E. maximum number of simultaneous TCP and/or UDP connections
F. fragments reassembly options

**Answer:** CDE